White Paper Security

Version 2.0

This document was created using AuthorIT™, Total Document Creation (http://www.author-it.com).

Disclaimer

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by DocuWare GmbH. DocuWare GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

DocuWare GmbH
Therese-Giehse-Platz 2
D-82110 Germering
www.docuware.com (http://www.docuware.com)

DocuWare

Contents

1 Introduction

DocuWare is a modern document management system for professional enterprise content management. DocuWare lets you access your documents and the important information they contain anytime, anyplace.

This white paper presents the security measures within the DocuWare software. We outline the features DocuWare offers for data safety, backup, prevention of failure and data loss, as well as the features for protecting communication and documents against misuse and manipulation. Therefore, a complex system of access rights and roles is included. Also the verification with an electronic signature and the traceability of events within the system and logging are discussed. It mentions the underlying technologies and describes how they are used by the DocuWare system.

This document is intended for clients (users), consultancy companies, IT magazines and distribution partners. It assumes a certain level of technical knowledge about the structure of software applications, ideally of document management systems.

Please find detailed information about the DocuWare system and its components in the White Paper System Architecture (http://help.docuware.com/en/#t61104). For questions about terminology, please consult the glossary at the end of the document.

2 Access Security

To prevent abusive access to the stored data DocuWare can be protected by encryption of the data transfer and various login methods.

2.1 Overview System Architecture and Protocols for Communication

A DocuWare system consists of several client and server components. They are organized in three layers.

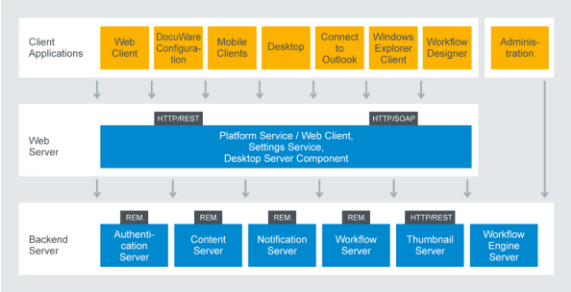

Figure 1

You can find more information about the communication technology used in DocuWare in the White Paper System Architecture http://help.docuware.com/en/#t61139.

DocuWare works with open communication standards and uses HTTP/HTTPS between very many components, mostly either together with REST (Representational State Transfer) or SOAP (Simple Object Access Protocol).

In particular, the DocuWare Platform Service is fully REST-based. SOAP is for sharing messages based on the XML Information Set. In the DocuWare System, SOAP is used by various web servers for communication with client applications.

The servers communicate partly with TCP respective Remote.

To prevent attacks it is important to secure the communication with HTTP between the web-based client applications and the Platform Service with SSL.

The DocuWare Administration is the only client application, which can communicate directly with the servers with TCP. In this case the encryption of TCP is used.

By default, the encryption of the protocols is disabled. The system administrator however can activate the security protocols for each in- or outgoing server connection.

2.1.1 HTTP Encryption

To protect the data traffic between the client applications and the Platform Service HTTP should be encrypted with SSL (HTTPs) at any rate. In order to do this, a certificate must be created in the Internet Information Server. Certain components of the system need to be reconfigured then.

To configure the DocuWare Web components for HTTPS (SSL), you must carry out the following steps in IIS manager:

- Import the certificate or certificates ("server certificate", "Import" action)
- Adapt the website link and make it accessible via SSL
- If necessary, remove the HTTP link for security reasons (optional)

If you use a self-signed certificate, you must also ensure that your certification center is defined as a trusted certification center on all clients. To do so, import the certificate into the certificate store of all computer and user accounts in your domain, for example using a Group Policy Object (GPO) from Microsoft.

More information is available in DocuWare Support (http://www.docuware.com/support_faq/?action=search&search=ssl+zertifikat&submit.x=0&submit.y=0).

2.1.2 TCP Encryption

The settings of TCP-based communication of some of the servers respective of the DocuWare Administration and the servers can be changed in DocuWare Administration, for example in the server settings. For each communication channel you can apply different security levels, ie. "SSL," or "Windows security." By default "No security" is applied.

We recommend SSL encryption for communication outside of domains and via public access channels. For SSL communication servers must have an appropriate certificate that is deposited in the Windows certificate store of the particular computer.

"Windows Security" is applied, when client and servers are located in the Intranet. The supported protocols with "Windows Security" are Microsoft NTLM and Kerberos. We recommend Kerberos because of its superior security. Only in cases where the partner system does not support this – for example, older Windows versions – is NTLM used for compatibility reasons.

Kerberos is a so-called "Ticket Granting Protocol" (see also Access Security (on page 8)). Developed by MIT in Boston; Kerberos is an IETF standard and widely supported.

DocuWare Support provides you with more information about configuring Kerberos (http://www.docuware.com/support_faq/index.php?action=artikel&cat=7&id=1319&artlang=de&highlight=kerberos).

2.2 Login

2.2.1 Login methods

The login to DocuWare is always verified via Authentication Server. The login procedure also incorporates a verification of the licenses available to the user. The following user authentication methods are supported by Authentication Server:

- **DocuWare-Login**
  Users must prove their authorization by means of the name and password as stored in DocuWare.
- **Trusted Login (Single-Sign-On)**
  The client is identified without any other user input by using the credentials of the current Windows operating system session. Authentication Server verifies these credentials directly. This method also permits cooperation with other single sign-on systems. The directory services based on LDAP and Active Directory are supported.
  This method is not available in all scenarios. Trusted login can only be used if client and server are located in the same Windows domain network. With the trend towards mobile devices and centrally hosted solutions, this type of login will become less popular. It is not available for DocuWare Online.
- **Login Token**
  Tokens are an internal logon mechanism which is mainly used for Single-Sign-On between different DocuWare components. For this purpose, the Authentication server issues tokens to an already authenticated user in application A. The token is then passed in a secure way to application B which can in turn use the token to authenticate with Authentication Server. So the user has, for example, not to log in again, if he uses first Web Client and then Web Client Settings.

2.2.2 Login via HTTP

All components connected over HTTP connections apply a cookie-based mechanism: Credentials once validated are stored in encrypted form in a session cookie. This authentication cookie will be used, if authentication is required again, e.g., reopening the browser.

As the Authentication Server is not available over HTTP directly, login requests of HTTP-connected applications are always processed over the middle tier of Web Client Server or Platform Service. This component then forwards login credentials to Authentication Server. After successful authentication, a cookie is provided to the client as part of the HTTP response. This cookie is used in subsequent requests.

Proxy servers and firewalls may also be interposed, although they have no further influence on login procedure as explained here. Provided that the clients are connected over HTTPS, transferred credentials cannot be intercepted on the way.

2.2.3 Login over TCP connections

For the components communicating over TCP, DocuWare uses a "ticket-granting-ticket" (TGT) system, whereby a user or client identifies themselves to Authentication Server, requests a service, and is given a "ticket" which then allows them to use the service of another server, for example of a Content Server. Authentication Server(s) have central

control function over the "sessions" within the system and can on the one hand impose the security features and on the other react proactively in the event of failure or overload of individual servers.

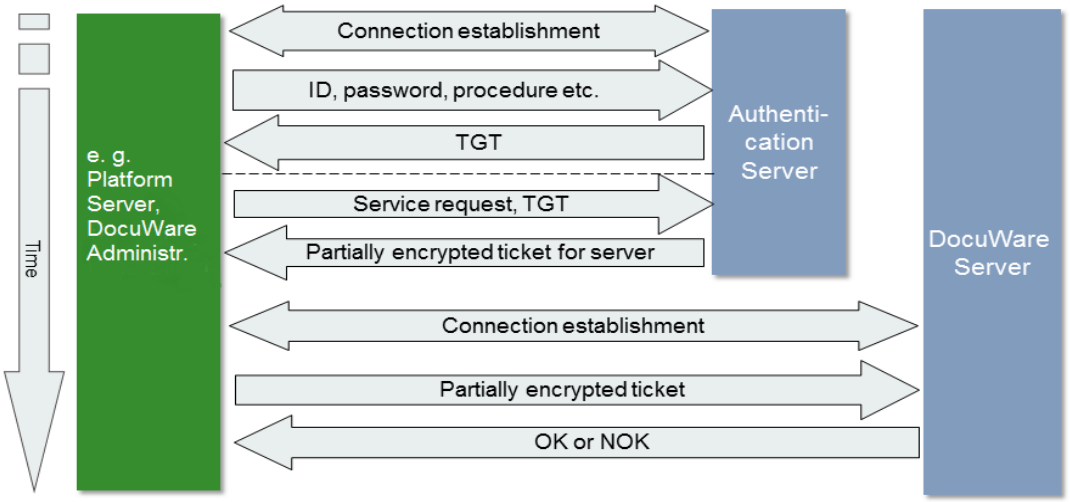

Figure 2: The login-process of a DocuWare system in detail. A ticket grants security.

The authentication processes shown in the illustration is described in four steps below.

2.2.3.1 Step 1: Client Login to Authentication Server

General login procedure for Authentication Server:

1 Platform Service (or DocuWare Administration) establishes a secure, encrypted communication connection with Authentication Server.

2 DocuWare login only: Platform Service asks the user for the user name and password.

3 Platform Service identifies itself to Authentication Server using account name and password.

4 Authentication Server checks the information, creates a "Ticket-Granting-Ticket" (TGT) and sends it to the Platform Service. It also notes the license usage. Depending on which application logs on, one license is blocked until logout or timeout.

2.2.3.2 Step 2: Client Service Request to Authentication Server

Once logged on, the Platform Service (or DocuWare Administration) can request the use of services from Authentication Server using the following procedure:

1 the Platform Service (or DocuWare Administration) submits the following information to Authentication Server:
a. Required backend server type, i. e. Content Server, Workflow Server or other servers
b. Additional required parameters, for example identification of the logical file cabinet
c.The TGT received above

2 Authentication Server determines the server to be used, according to the configured load balancing method.

3 Finally, Authentication Server sends the Platform Service (or DocuWare Administration) a time-limited ticket for this server. The ticket includes a session key for communication between client and server.

2.2.3.3 Step 3: Client Login to Assigned Server

the Platform Service (or DocuWare Administration) now uses this ticket to log on to the server assigned by Authentication Server. The procedure is as follows:

1 the Platform Service (or DocuWare Administration) establishes a secure connection to the server to be used and submits the ticket received from Authentication Server.

2 Server evaluates the information contained in the ticket and checks the ticket's validity.

3 Server sends confirmation to the Platform Service (or DocuWare Administration) and is now ready to receive requests.

If the ticket has expired, it is up to the Platform Service to request an extension of the ticket from Authentication Server. The procedure is similar to requesting a new ticket. However, since the same session key is used, the session can be continued without loss.

2.2.3.4 Step 4: Client Logout from Authentication Server

At the end of a session, the Platform Service must log out of Authentication Server in an orderly fashion. The Platform Service establishes a secure connection to Authentication Server and submits the Ticket-Granting-Ticket. Authentication Server then releases the license again.

Licenses can only be used for a defined period. If the Platform Service fails, the license is freed by a timeout. After a failure and restart of Authentication Server, blocked licenses are also released.

2.2.4 DocuWare Passwords

Credentials are generally encrypted in DocuWare. The same is true for system settings as for example the login to the database server.

Technical implementation

DocuWare passwords are generally stored only in a hashed form. It uses the "salted" hash procedure, whereby a random value ensures that even two identical passwords do not generate the same hash value. This means that passwords can neither be read nor reproduced.

If a user should forget his password, he or she can demand a new, automatically generated password sent by email via a link in the login dialog of the Web Client. The user can use this to log on to Web Client and set up a new personal password.

Alternatively the organization administrator can reset the password. However, this is not possible for high-security-users. These users have to restore their password for themselves (also see the chapter High Security Systems (on page 19).

User settings

The complexity of passwords within the organization can be specified in DocuWare Administration. For example, passwords must then have at least one capital letter, one lower-case letter, one number and/or one special character. In addition, you can define the minimum length of the password, how many days it remains valid and how many incorrect entries are possible before the user account is locked, and much more.

The administrator of the organisation can disable the password time limit again for individual users. This is particularly useful for users that are only used for workflow processes in DocuWare.

2.2.5 Credentials for other systems

All sensitive information (credentials for other systems, such as database server password, mail server password, LDAP passwords etc.) is always stored in an encrypted form that only the server components can decrypt.

This is to keep them secure, even if you have users that have access to the database such as backup operators.

3 Rights Management

Employees in large organizations deal with complex processes and are subject to a variety of rules and regulations. In order to carry out their tasks they need authorization to use particular resources such as document and IT functions. Certain restrictions make sure that only authorized personnel have the right to do certain things, and maintain transparency for everyone.

DocuWare uses a rights concept which allows you to define in great detail, for each DocuWare user, which activities he or she can perform within the DocuWare system.

3.1 Terminology

3.1.1 Rights

An essential element of rights administration in DocuWare is the distinction between functional rights and file cabinet rights. In addition, rights can be specified for some objects.

- **Functional Rights**
  A user can be assigned various functional rights. These can include managing dialogs in the Web Client, managing Baskets, Email-Notifications in DocuWare Configuration, and many more.
- **File Cabinet Rights**
  File cabinet rights specify which access options a user has to file cabinets, that is to say documents and index data. These rights include storing and retrieving documents, editing index entries or exporting stored documents to the file system. A user can be assigned various file cabinet rights for each file cabinet.
- **Usage and administrative rights**
  Some types of objects can be assigned to users and roles, including Baskets, OCR Settings, Smart Connect Configurations, Import Configurations and more. Such an assignment can be a usage grant or an administrative grant. The user can use the configuration or the basket, administrative grant permits to change it.

The total of all a user's functional rights, file cabinet rights and object rights constitute this user's activity scope.

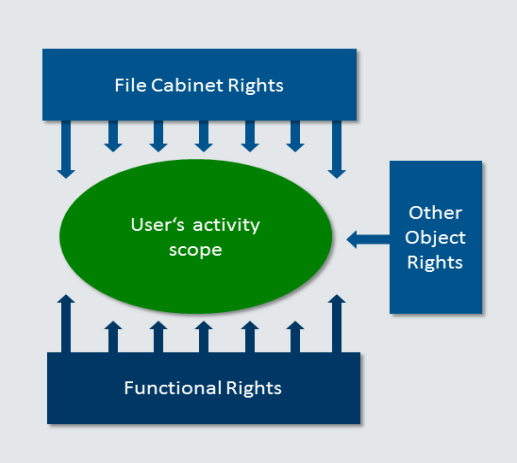

Figure 3: Thanks to a complex rights-structure, the user's activity scope can be determined in detail.

3.1.2 Profiles and Roles

Profiles and roles enable you to assign sets of rights in "containers," instead of a lot of individual rights. The assignment of rights to profiles and roles has two advantages:

First, detailed sets of rights can be assigned at the touch of a button to as many users as required, without the administrator having to customize the rights structure manually for each user.

Second, sets of rights also exist without users, so when an employee leaves the company, their successor can be effortlessly assigned the same rights, regardless of how specific the rights assignment is.

- **Profiles**
  Rights can be combined as functional or as file cabinet profiles. Both can be assigned to individual users and roles.
- **Roles**
  Roles are sets of several profiles. A role can include both profiles with functional rights and profiles with file cabinet rights. Roles can be assigned to groups and to individual users.

3.1.3 Users and User Groups

Individual DocuWare users can be combined into different groups. A user can be a member of more than one group.

- **User**
  As a rule, one user is created for each staff member who needs to work with DocuWare. Users receive a range of rights through the assignment of individual rights or sets of rights in the form of profiles and roles. Users can belong to groups.
- **Groups**
  Groups are sets of users. It is a good idea to combine users into groups which need to use the same program functionalities and be assigned the same file cabinet rights. Individual users receive these rights through their membership of the group, to which the appropriate role has been assigned.

3.1.4 Inherited Rights and Explicit Rights

When assigning rights to users, DocuWare distinguishes between inherited rights and explicit rights.

- **Inherited Right**
  Rights that a user has received through membership of a group or through a role or a profile are called inherited rights.
- **Explicit Right**
  Rights which a user receives directly (and not via a role, profile, or group), are explicit rights. Only functional rights and usage and administrative rights in the configurations in DocuWare Configuration can be assigned as explicit rights.

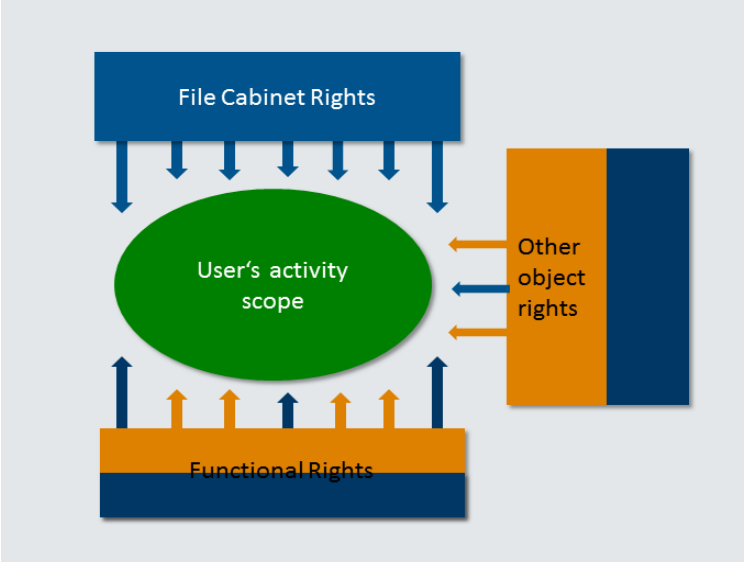

Figure 4: Explicit Rights, here marked orange, are assigned directly to users. Or the user inherits a right from a role or a group (blue).

3.2 Assigning Rights

DocuWare provides the described variants of assigning rights, so that administrators can choose the one which is best suited to their organization. Groups (as sets of users) and roles (as sets of rights) are different ways of looking at one and the same thing. From one perspective, the employees are the starting point. From the other, the starting point is the workflows and functions in the DocuWare system.

3.2.1 Assigning Functional Rights

Functional rights are used to determine which menu items are available to a DocuWare user in the Web Client, in the DocuWare Configuration and Workflow Manager. They also determine part of the user's activity scope in DocuWare Administration.

The assignment of individual menu functions as rights allows you to define precisely which functionalities are available to a user within the DocuWare system or not. For example, if an employee is not allowed to manage Baskets, the module will not be displayed when the user calls up the DocuWare Configuration.

3.2.2 Assigning File Cabinet Rights

File cabinet rights are always combined into profiles, meaning, they cannot be assigned directly to individual users. Only file cabinet profiles can be assigned to users or roles.

As with functional rights, file cabinet profiles are also additive. If several profiles of a file cabinet are assigned to a user, this user receives all the rights that are shared by these profiles. This procedure is explained in more detail in section Interaction of rights (on page 18).

File cabinet rights can be further distinguished: administrative and general file cabinet rights on one hand, and in field rights on the other hand.

- **Administrative and general file cabinet rights**
  Administrative file cabinet rights include the right to: modify file cabinet rights for users, create search and store dialogs and result lists for this file cabinet, and migrate the file cabinet. General file cabinet rights include the right to store, retrieve, and delete documents.
  File cabinet rights always relate to one file cabinet along with all the documents it contains. Different file cabinet rights can be assigned to different file cabinets.
- **Field rights**
  In addition to general file cabinet rights, rights can also be assigned at field level. These rights relate only to the specific field, not to all fields of a file cabinet. Field rights include the right to retrieve, to modify field contents, plus the right to use entries that are not available in a select list.

(With index filters you can fine-tune rights in more detail. Index filters can be used to select specific documents by their index entries. Limiting access to documents by means of index data is particularly useful when documents containing sensitive data are grouped together in a file cabinet. For example, documents relating to employees are stored in an HR file cabinet. The employee name is one of the index entries available. HR department employees have access to all documents, while individual employees can only access those documents that have been stored with their own name in the index data.)

3.2.3 Assigning Administrative and Usage Rights

First, it is necessary to assign the functional right to manage the module in question in DocuWare Administration to a user. The administrator can assign to user x the right to manage, for example, OCR Settings. Then the module OCR Settings is displayed in the DocuWare Configuration, when user x logs in. User x can now apply a new OCR setting and determine, which user or groups shall work with or to administrate this setting.

3.2.4 Predefined Roles

After the initial installation, each DocuWare system contains predefined roles with predefined profiles; this means that administrative tasks are also subject to the authorization concept. These predefined roles can be assigned to different users or user groups.

System Administrator

The system administrator manages the system with regard to the hardware and the basic components which are generally needed. This includes managing the database connections, plus the administration of communication paths and document storage paths.

The system administrator can be defined so that he or she cannot access individual organizational data, and specifically cannot intervene in the details of the user administration. However, only he/she can assign the "System Administrator" role to other users. This cannot be done within the organization's user administration.

After DocuWare has been installed, he/she assumes the role of organization administrator for all organizations simultaneously. As each new organization is created, the system administrator initially automatically assumes the role of organization administrator. This can then be assigned to another person.

System Administrator Tasks

- Hardware, operating system, database
- Installing und updating DocuWare server modules
- Configuring system-wide settings for:
- Server as Authentication Server, Content Server etc.
- Connections as databases, data files, SAP remote connections, time stamp services etc.
- Storage systems
- User directories
- Logging

Organization Administrator

A DocuWare system can include one or more organizations, each with its own organization administrator. The organization administrator manages in particular the rights, users and user groups of their organization. The role does not include access rights to file cabinets and their administration.

This role does not require any detailed technical knowledge of the IT environment. The organization administrator can also assign or remove the role to and from other users. In particular, the role can even be removed from a system administrator.

Organization Administrator Tasks

- Licences
- Clients and baskets
- Stamps
- Viewer and external applications
- Select lists
- Validations
- Users and groups
- Logging
- Workflows

File Cabinet Owner

The right of the file cabinet owner is automatically assigned by the DocuWare system to the person who creates the file cabinet. He or she can then assign this right along with other rights for carrying out administration tasks to other users.

The owner manages the file cabinet structure, e.g. index and disk structure, and assigns the access rights to the file cabinet in which he or she creates file cabinet profiles. With reference to the file cabinet, the owner also defines the settings for the organization administrator, so that the latter can assign the file cabinet profiles to users and/or roles.

File Cabinet Owner Tasks (per file cabinet)

- *Full text indexing*
- *Used database connection*
- *Document storage and disk concept*
- *Index fields*
- *Rights to file cabinet*
- *Dialogs for storage, retrieval and result list*
- *Logging*

3.2.5 Object Rights: User or administrator

For a number of other objects, users and roles can be granted "usage" and "admin" rights. Usage right of, for example, a configuration of baskets in the DocuWare Configuration usually means that the respective user or role can use the configuration, but not change the settings. Admin rights usually means, that the user can even change the object, but not use it. It is possible to assign both rights to a user, so that he or she can use and change a configuration.

Objects where this system is used:

- *Baskets*
- *Smart Connect*
- *Email Notifications*
- *MFP Workflows*
- *OCR Templates*
- *Connect to Outlook*
- *Import*
- *Printer*
- *Connect to Mail*
- *DocuWare Request*
- *DocuWare Forms*

3.2.6 Interaction of Rights and Authorizations

Member of several groups, owner of several roles or profiles

Rights are always additive, in other words, the total of all a DocuWare user's assigned rights constitute this user's activity scope.

If a user is a member of several groups, he or she has all the rights that are available through assignment to these groups and their roles.
If several roles or profiles are assigned to a user, this user has all the rights that have been assigned to these roles or profiles.

Examples:

- A user has received his set of rights via a role. If you now assign this user an additional role that has fewer rights, it does not change anything for that user, since rights are additive. In order to restrict his rights, you would have to remove the original role from him.
  (The same applies to groups.)
- A user is a member of two groups and has received his set of rights via the roles of these groups. If you now remove the membership of one group from him, he does not automatically lose all the rights that are assigned to him via the roles of this group, but only those that are not assigned via the other group.

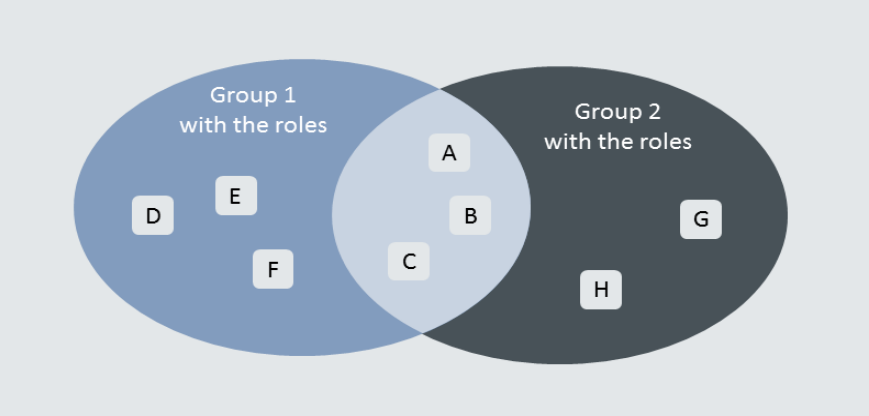

Figure 5: If you remove the membership of group 2 from a user, he only loses roles G and H, as he still has roles A, B and C via group 1. The same applies also to roles and profiles assigned to a user.

Functional Rights and File Cabinet Rights

File cabinet and functional rights are assigned independently of one another. However, for a logical rights canon, they should not necessarily always be viewed as independent of each other. Here is an example:

- For a user to be able to search in file cabinet, he needs the Search right and a search dialog assigned to him at file cabinet level. Under functional rights he also requires the Search functional right; otherwise he will not be able to open the search dialog. The same applies for storing documents in a file cabinet.

Dialog Settings and File Cabinet Rights

The options that a user has within a file cabinet result from the file cabinet rights, which also include the relevant dialogs. Here is an example:

- Two users have a result list which provides the "Download a PDF with annotations" button in its toolbar. One user has the Export-file cabinet right and can make use of this option. The other has not been given this right. The "Download a PDF with annotations" button is greyed out then and the user cannot make use of it.

Field Settings and File Cabinet Rights

The settings for the individual file cabinet fields and assigned file cabinet rights overlap in some areas. It is therefore possible to make special rights available to designated users, while "normal" user rights are controlled by means of field settings. An example:

- A file cabinet field has been specified as a Fixed value in the Store dialog, and a user has the right to modify index entries. This user is authorized to change the fixed field entry in the Store dialog and/or in the Info box of the result list.

Summary: a user's file cabinet rights always override the field rights. Using a combination of both schemes should therefore be done with care.

3.3 DocuWare as a High Security System

You can change a DocuWare System into a "high security system." The organization administrator can then assign the high-security-property to certain users and file cabinets. Only a high-security-user can access a high-security-file cabinet. There are some differences from a normal system:

- A user with the high-security-property, the password can no longer be reset by the organization administrator. Only the users themselves can change their password.
- A high-security user cannot log on using a trusted login (see Chapter Login methods (on page 8)), since with trusted login security is not ensured by DocuWare.
- If a file cabinet is set to "high security," it is no longer possible to assign file cabinet profiles to roles for these file cabinets, since file cabinet profiles must be assigned directly to users. These users must have the "high security" property. This prevents access to especially sensitive areas being granted by accident through uncontrolled groups and role assignments.

4 File Cabinet Security Mechanisms

In addition to the authentication system and the authorization concept, other measures exist for protecting file cabinets against misuse and inconsistencies. These include a transaction procedure in Content Server, locking documents that are being revised, tracking changes of a document, encrypting file cabinets and a simple backup of documents by synchronizing file cabinets.

4.1 Content Server Transactions for data consistency

The operation of saving documents, which causes a number of updates both in the database and the file store, has been implemented in Content Server as a transaction, thus ensuring the consistency of the system. If certain steps of such a transaction cannot be completed, the changes made are discarded automatically in a rollback. The database and the file store contain the same information.

4.2 Locking Documents in File Cabinets

To prevent two users from editing a document at the same time, it is possible to lock documents. Other users can still view the document, but they cannot set annotations or stamps. In DocuWare Administration you can determine the mode in which the Web Client viewer opens and displays a document from the result list. The following modes are possible:

- Edit Mode: If a document is opened in this mode, it can be edited. It is locked for other users in the file cabinet as soon as it is displayed. The lock is removed as soon as the document is closed.
- Ad-Hoc-Edit Mode: This mode is set by default. The documents are initially opened in read-only mode and are not locked in the file cabinet. As soon as the user selects an editing tool, the document is released for editing and locked in the file cabinet.
- Ready only: A document can be viewed, but not edited. Comments or stamps cannot be applied.

All locking data is recorded in the database. Special mechanisms ensure that locked and released documents are always restored to a consistent state, even after a failure of the client, the application, or even the server.

4.3 Version Management: Tracking of Documents

If version management is enabled for a file cabinet, all changes to a document stored in this file cabinet can be tracked. When a document is edited, DocuWare saves the changes in a new version. The original and the older versions are retained in the file cabinet. The document being edited can be locked so that two users cannot accidentally work on a document at the same time.

There are two options for working with version management in DocuWare.

- Manual: The user checks out a document, either into the file system (Web Client and Windows Explorer Client) or into a basket (Web Client only). As soon as a document is

checked out of the file cabinet, it is locked in the file cabinet. Other users can view it in read-only mode. When checked into the file cabinet, the document receives a higher version number that the user can assign themselves. It is also possible to enter a comment for the new version.

- Automatic version management is active in the background without any manual intervention required from the user. The open document is locked during editing. Changes are saved in a new document with an automatic version number. You can also check out documents from file cabinets with automatic version management, but then it's moved to manual control.

With both variants of version management, the original and the older versions are kept in the file cabinet and can be seen in the version history. The version history shows the version numbers, the status, the storage date, any comments and the user who saved the document, among other things.

The status of a document makes it obvious which document version is which. This may be "Up to Date" for the most recent document, "In Progress" for a document that has been checked out or already opened in DocuWare, and "Out of Date" for a version that is no longer up to date.

The status changes automatically when a document is opened or checked out from a file cabinet with version management enabled in the original program. For manual version management, it is possible to change the status of a version from "Out of Date" or "In Progress" to "Up to Date". This may be necessary if a checked-out document is accidentally deleted, for example. However, only one version can have the "Up to Date" status at any one time.

4.4 Encrypted File Cabinets

To ensure that not even an administrator can read sensible documents, DocuWare offers an encrypted storing of documents. Optionally, the associated header files can also be encrypted.

Full text information is NOT encrypted by DocuWare (see also Chapter Protecting sensible data outside of DocuWare (on page 23). The index data in the database is also not encrypted. If the index data contains highly sensitive information, you should consult the options offered by the database provider.

Note that encrypted file cabinets can only be accessed by authorized users. The keys for decrypting the documents are stored in the document header. The document keys are decrypted using an asymmetric procedure with a key stored in the database. Since the documents cannot be decrypted without the key in the database, if you are using encrypted storage you should make sure that regular backups are made of the DocuWare system tables, so that the key tables in particular can be restored if the database is lost.

4.5 Backup of a File Cabinet with Synchronization

DocuWare permits the synchronization of two file cabinets, making it possible to store documents in two or more DocuWare systems at a time, for example to compile a backup.

The synchronization includes both the documents and the database. The starting point for synchronization is always the source file cabinet, e.g., the master file cabinet. The

destination is always a "satellite" file cabinet. This may be a DocuWare file cabinet on a laptop that needs to be able to work with the latest documents in a master file cabinet without having access to the network.

The master and satellite file cabinets can have different structures. The database fields can be assigned when you define the workflow. All the documents or only a few selected documents can be copied from a file cabinet into the satellite file cabinet. There are some highly detailed filter functions you can use to specify which documents are to be synchronized.

Basically, synchronization works in both directions: Documents in the master file cabinet can be transferred to the satellite file cabinet. In the other direction, changes to documents or new documents in the satellite file cabinet can be transferred to the master file cabinet. The documents in the satellite file cabinet are given their own DocID, which corresponds to the logic of the file cabinet; they also receive the DocID of the master file cabinet. This makes it easy to synchronize satellites with the master file cabinet.

In order to use the Synchronization workflow for documents with enabled version management, version management must be enabled with the same settings for the master and the satellite file cabinet. Otherwise the synchronisation job won’t start. New document versions can only be created in the master file cabinet. In the satellite file cabinet, documents are write-protected with version management. To transfer a new version to the satellite file cabinet, you must synchronize the file cabinets.

4.6 Protecting sensitive data outside of DocuWare

If you work with DocuWare, some of the data is unshielded and cannot be protected by specific DocuWare security mechanisms.

This include the index data of the documents, the extracted full text, or the thumbnails of the documents created by Thumbnail Server for displaying in Web Client, all of which are stored in their respective databases. Every system administrator with sufficient privileges to view the database can access these data.

Full text is also stored in a separate index that is controlled by the full text server. The full text server is based on Apache SolR, a widely used full text engine.

If these data repositories contain sensitive data, then access to the databases, to the index location, and the access to the full text server URL - by default http://machinename:9012/solrt (http://machinename:9012/solrt) need to be restricted by the administrator using common methods such as access control lists for file directories or databases.

4.7 Electronic Signatures

With an electronic signature it is possible to verify the writer of a document. Also modifications of signed documents can be detected.

In DocuWare, PDF signatures are applied using these certificates from the Windows certificate store. The owner of the private key adds the signature and the receiver of document can verify the sender with a public key, which is in most cases stored on the client workstation.

In DocuWare, electronics signatures can be added to scanned documents in DocuWare Scan or to documents, which are imported with the module DocuWare Import .

5 Fail-Safety

A failure of a document management system in a heterogeneous IT structure may have multiple causes. To prevent data loss and technical problems we recommend solutions for server platforms that address this problem including "clustered" systems which not only offer improved fail-safety, but also provide load balancing between them.

DocuWare Server can deal with clustered systems, as Authentication Server (http://help.docuware.com/en/#t59877) stores all settings in the database, and it works in a "stateless" fashion, which means that no data are stored temporarily within an application. In this way, Authentication Server can make unrestricted use of the underlying server platforms. It can also run on a system that is composed of several computers. Content Server on the other hand works in a "stateful" manner.

But provided that several Content Server (http://help.docuware.com/en/#t59877) run in parallel on the various systems, they can also benefit from the additional performance and enhanced security of these platforms.

Sophisticated procedures are also available for database servers. We recommend using these options, given the significance of the database for the DocuWare system. As far as storage technologies such as RAID drives are concerned DocuWare can make use of such technologies, but have no influence on these components.

DocuWare provides secure communication and transaction procedures. The sophisticated identity checks for users and systems among themselves (see Access security (http://help.docuware.com/en/#t59877)) also increase system availability, as these prevent downtimes caused by deliberate or grossly negligent behavior.

The following sections describe in more detail those aspects that DocuWare contributes to fail-safety; we do not here touch further on the options afforded by the platforms.

5.1 Preventing Failure of DocuWare Server

Installing redundant DocuWare servers makes sure that the DocuWare application is constantly available.

If, for example, an Authentication Server no longer responds, the Platform Service contacts the next Authentication Server. However, this does not occur automatically; instead, the user logs in again. For this purpose, a sequence of Authentication Servers can be configured on the client. When a new login occurs, all Authentication Servers are checked for their availability, one after the other. The same applies to DocuWare servers, which also need to login to Authentication Server in order to obtain a ticket for their operation.

After the authentication of the user and the license check, Authentication Server allocates the required and available servers to the user. If a Content Server does not answer to Authentication Server, the client requests a new service. Now the failing Content Server can be by-passed by a redundant Content Server.

Because the Content Server works in a transaction-oriented way, changes to the databases become effective only with the concluding "Commit" command. If this command is not issued due to a server failure, the original state prevails. This prevents an inconsistency in the system; see also Chapter File Cabinet Security Mechanisms (on page 21).

Also for most of the other server modules failover mechanisms are available. Please ask the DocuWare Support for more information.

You can find more Information about failover of DocuWare systems in the White Paper System Architecture in the section Scalability http://help.docuware.com/en/#t60980.

5.2 Protect System Database

As all rights and licenses are stored in the system database DWSYSTEM, it is important to reduce the possibility of failure or misuse to a minimum.

- Only Authentication Server accesses the DWSYSTEM. To achieve maximum security, Authentication Server works via its own database account, so there is only one "user" who has direct access to this database. The client does not have direct access to the Authentication Server database, only to the interface of the appropriate Authentication Server plus the Backup Authentication Server.

5.3 Recovery

To access stored documents you need the index data in the database DWDATA. Without this information, Content Server cannot find the documents on the storage system. In case of data loss, the backup copies of the databases and documents ought to enable you to restore the system and file cabinet to the state they were in at the time of the most recent backup.

Even for a situation where the backup copies of the database DWDATA are not available or are corrupt, DocuWare offers a possibility to restore data. Of course, the recovery of large file cabinets can take a lot of time.

In order to restore index data DocuWare uses the principle of "double data retention". This works by writing an additional copy of the index data for each document into the XML header file. The required document stores must be available during the recovery operation. You can restore the data with a Restore Workflow.

To restore a corrupt database, DocuWare needs the following information:

- the database fields, e.g., the structure of the database
- the file cabinet paths of the document files
- the index information for the stored documents

DocuWare can even restore encrypted file cabinets. The document encryption key is written into an additional file in the storage location next to document header. A second key, the file cabinet key, is stored in the DWSystem. It is used to encrypt/decrypt the documents key.

A special challenge arises in cases where on account of revision-proof archi ving requirements, documents and XML files were stored at a very early stage to non-modifiable storage media (e.g. WORM). In such a case it may not be possible to completely restore the index data, since changes that were made after the backup operation are no longer available because they could not be updated in the header (header was write-protected).

6 Backup

Backup operations should be in place for the data and documents within the DocuWare system, just as for any environment. These are the components to be backed up.

6.1 System configuration: DWSYSTEM

All system and organization relevant properties are stored in the DWSYSTEM database which is accessed by Authentication Server. We recommend that this database be backed up at least once a week, but certainly after any extensive changes.

6.2 DWDATA and Documents

The data in the file cabinets are stored in the DWDATA database. During normal operation, this database ought to be backed as often as your security needs are.

In addition, the file cabinet contents themselves, e.g., the documents and associated XML files, must be backed up. This can be done using traditional procedures such as tape backups with "generation" procedures. However, it may be necessary to consider the very large data volumes in file cabinets which may not make it practical to use full backup. In such cases, incremental backups are usually preferable, as this method will keep the data volumes to a manageable level.

If removable storage media (optical) are used, creating manual copies of the production media might be the simplest solution. Depending on the storage sub-system it may be possible to automatically create parallel backup media. Certain sub-systems implement redundant storage procedures or automatic mirroring, which to a large extent take the place of traditional backup procedures.

DocuWare functions can be used for backup purposes, too. File cabinets including associated index data can be copied via the export options into other file cabinets and thus act as backups.

It is worth considering also that the creation of master/satellite file cabinets provides a comfortable option to resolve the backup problem without any manual intervention. Synchronization can then be used to automatically update the backup copy. What you need is sufficient storage and transmission capacity in the infrastructure.

Thus, you might set up a satellite file cabinet purely for backup purposes at another connected site, and then synchronize this automatically with the master file cabinet, for example every night.

6.3 Worfklow Engine Database

Workflow Engine uses a separate database, DWWORKFLOWENGINE, containing all information for Workflow Manager including configuration and workflow history. It has to be backed up too, as Workflow content is not stored in the document headers.

6.4 Other DocuWare Servers

Fulltext Server has its own index files, which can be backed up too. However, the creation of index files is very fast, so it would be a minor problem to lose them. Notification Server uses a separate database, which needs to be backed up separately in order not to lose information about notifications.

To save time after a potential crash, the full text index and the thumbnail database should be considered to be backed up.

7 Logging

DocuWare provides a flexible logging function for recording all relevant events. This serves as an optimal support mechanism for identifying the causes of any problems and for system monitoring purposes.

7.1 Log types

Each DocuWare server module is responsible for logging its activities. Depending on the rules that have been set up and the server module, administrators can selectively enable and disable logging functions.

Logging functions are subject to the DocuWare rights administration. In the same way as administrator roles, the following logs have been set up and must be configured by the administrators:

- System log
- Organization log
- File cabinet log

In addition, special logs are available for the predefined workflows in order to provide elegant monitoring for these automated processes.

The logging function can be customized to suit the requirements of a company. A wizard assists with the configuration. The usual procedure for defining a log includes these steps:

1 Definition of relevant events and target formats

2 Definition of the objects to be logged

3 Specification of the information to be logged

4 Definition of filters (e.g., if events are to be logged only if they were triggered by a particular user)

First, you decide what type of event (logging level) is to be recorded where. Then you specify the log content with the relevant objects and the information to be logged.

7.2 Logging Levels

For logging, you have a choice of different target formats (database, XML file, formatted file) and different events (information, warning, error, critical error). A lower level includes the events of a higher level. This means that enabling the "Information" level will produce a log of all events.

Errors of the "Error" and "Critical error" levels can automatically be added to the Windows log. These cases also permit automatic sending out of e-mails.

Events and their significance:

Critical error:
An unexpected error for which there is no standard handling routine.

Error:
Error for which handling routines exist, for example if a particular document cannot be accessed.

Warning:
An operation could not be performed, but the workflow is not adversely affected, for example: missing rights for writing index data.

Information:
Additional information on events that might be interesting for administrators.

Each event that causes a deviation from the planned sequence can generate an entry in the log. This means that logs capturing all events at runtime can become very large, thus adding to the system load. For this reason, you are advised not to log anything but errors during normal operation (see also predefined logging (on page 32)) and to enable additional information only during troubleshooting.

For audit purposes you can use comprehensive logging at file cabinet level, for example if you wish to track changes of index data in the log.

7.3 Log Content

Events that are relevant for logging purposes are changes to the configuration by the administrators on the one hand and events that occur during runtime on the other. Logging of course does not contain any critical or user specific data as for example passwords.

Administrative events that are generally logged are the creation, modification and deletion of defined objects. The following table lists the objects that are logged during administration.

System level	Organization level	File cabinet level
▪ Authentication Server ▪ Content Server ▪ Workflow Server ▪ Connections ▪ Storage locations ▪ External user directory	▪ Licenses ▪ Private and public stamps ▪ Viewers and editors ▪ External select lists ▪ Validations ▪ Miscellaneous settings ▪ User synchronization ▪ User administration ▪ Signature types ▪ Workflows: ▪ File cabinet synchronization ▪ Export ▪ Migration ▪ Converting DocuWare-4 file cabinet	▪ General ▪ Database ▪ Documents ▪ Disks ▪ File cabinet profiles ▪ Search dialogs ▪ Store dialogs ▪ Result lists ▪ Link

System level	Organization level	File cabinet level
	▪ Restoring index ▪ Full text service ▪ Autoindex ▪ DocuWare Request ▪ Deletion ▪ SAP barcode transfer	

Table 1: Object types for logging within Administration

The log entry comprises:

- Name of setting
- Object type
- GUID

User making the change, with name and organization

A filter can be used to further restrict the events to be logged. This allows one, at system level, to filter organizations, and at organization level, to filter file cabinets and users.

	System level	Organization level	File cabinet level
Events	Open and Close	Open and Close	Open, Modify and Close
Objects	▪ Authentication Server ▪ Content Server ▪ Database connection ▪ Storage location ▪ External user directory	▪ File cabinet synchronization ▪ Export ▪ Migration ▪ Converting DocuWare-4 file cabinet ▪ Restoring index ▪ Full text service ▪ Autoindex ▪ DocuWare Request ▪ Deletion ▪ SAP barcode transfer	▪ Document ▪ Search dialogs
Object filters	▪ Organization ▪ Server name	▪ File cabinet ▪ User	▪ User
Logged information	▪ Name ▪ Object type ▪ GUID ▪ User, with name and organization	▪ Name ▪ Object type ▪ GUID ▪ User, with name and organization	▪ Name ▪ DocID ▪ Index information ▪ File cabinet name ▪ GUID ▪ User, with name and

	System level	Organization level	File cabinet level
			organization

Table 2: Logging during runtime

At every level (system, organization, file cabinet) several logs can be created at the same time.

7.4 Storage Location and Scope

The system administrator can define settings for the data sinks to be used, the database connections or file directories. He/she can also define the maximum size of the log file. When the maximum size is reached, DocuWare should create a new log file. This improves performance by overwriting the old log files.

The limits and the size of the areas to be overwritten can be selected freely. In the case of databases or XML files as storage locations, maximum size is indicated as number of records, otherwise as number of MB.

When creating new files on reaching the maximum, you can indicate a new maximum size.

7.5 Access to logging data

The option for specifying the logging mechanism is, just like other functions, subject to the authorization concept. This provides a special right for creating and deleting logging specifications ("logging agents").

The administrator who defines a storage location for the logs can indicate whether this location may be used by other administrators, or not. If not, then only he/she can define log specifications using this storage location.

A log can only be viewed by users that have the necessary administration rights for that particular level. Thus, an organization administrator cannot necessarily view the log of a file cabinet, unless he/she has the administrator rights for it.

7.6 Predefined Logging

Even without any user-defined logs, certain events within the system should be recorded. To ensure this, a specification is automatically set up during installation for one log each for the system, the organization and the file cabinet levels.

When installing a new organization or a new file cabinet, these specifications are also installed by default. These are database tables with a total size of 10,000 entries maximum.

Predefined logging at system and organization level logs all errors (critical and non-critical). With file cabinets, logging includes runtime events at warning level and administrative events at error level.

Property	Default setting
General Information	

Property	Default setting
Name	DWArchiv<Archivname>
Status	started
Logging-Level	Error
Target	DWLOG_<Archivname>
Additional output devices	none
Administrative view	
Objects	Events
All settings	Create, modify, delete
View at runtime	
Objects	Events
Exceptions	
Document	Create, delete
Potential information	
Document name	
DocID	
Index information and changes	
File cabinet name, GUID	
User name	
User organization	
Filter	none

Table 3: Example: Default logging for a file cabinet

Property	Default setting
General Informationen	
Name	DWOrganisation<Organization_name>
Status	started

Property	Default setting
General Informationen	
Name	DWOrganisation<Organization_name>
Logging level	Error
Target	DWLOG_<organization_name>
Additional output devices	none
Administrative view	
Objects	Events
All settings	Create, modify, delete
View at runtime	
Objects	
Exceptions	
Potential informationen	
Settings name	
Type	
GUID	
User name	
User organization	
Filter	none

Table 4: Example: Default logging for an organization

Property	Default setting
General Informationen	
Name	DWSystem
Status	started
Logging level	Error
Target	DWLOG_SYSTEM

Property	Default setting
General Informationen	
Name	DWSystem
Additional output devices	none
Administrative view	
Objects	Events
All settings	Create, modify, delete
View at a runtime	
Objects	Events
Exceptions	
Authentication Server Session	Open, Close
Content Server Session	Open, Close
Database connection	Open
Workflow Server	Open, Close
Potential informationen	
Settings name	
Type	
GUID	
Short User Name	
User organization	
Filter	none

Table 5: Example: Default logging for the system

Wizards are provided for taking the user through the steps required for defining the logs.

There are default logs for all kinds of workflow, enabling detailed monitoring of such automatic processes.

8 References

The following documents provide additional information:

- White Paper Intelligence Indexing (http://help.docuware.com/en/#t59237)
- White Paper DocuWare Online (http://help.docuware.com/en/#t58812)
- White Paper System Architektur (http://help.docuware.com/en/#t61104)